Welcome to Software Assurance

Don’t Panic!

Sean Barnum



- Wide range of established practices such as:
  - Software assurance policy
  - Secure requirements review with misuse/abuse cases
  - Threat modeling
  - Architectural risk analysis
  - Secure code review
  - Risk-based security testing
  - Penetration testing
- Resources available with practice specifications
  - Build Security In website (DHS)
    - https://buildsecurityin.us-cert.gov/daisy/bsi/home.html/
  - Build Security In Maturity Model (BSIMM)
    - http://www.bsi-mm.com/
  - Software Security Engineering: A Guide for Project Managers (Book)
    - http://www.softwaresecurityengineering.com/

- Making Security Measurable (http://measurablesecurity.mitre.org/)
  (languages, enumerations, repositories)
  - CVE
  - CWE
  - CAPEC
  - MAEC
  - SAFES
  - CEE
  - CPE
  - OVAL
  - CCE
- Formal standards
  - ISO 15026, 15288, 12207, 18045, several in process
  - OMG Software Assurance Ecosystem
- Guidance
  - Acquisition Guidance
  - Common Body of Knowledge
  - SwA extensions for CMMI
  - Practical Measurement Framework

- Broad range of commercial and open source tools available
  - Static Analysis (source, binary, byte)
  - Application Penetration Testing
    - Web Application Penetration Testing
  - Data Security Analysis
  - Vulnerability Scanners
  - Fuzzers
  - Configuration checkers
- Tools are NOT a silver bullet but are necessary to effectively support SwA practices and processes

- Private industry
  - Over 100 major organizations with strategic SwA programs
  - Large percentage with at least emerging tactical efforts
- Government
  - DoD
    - Various tactical efforts in NSA IAD
    - OSD
    - USAF Application Software Assurance Center of Excellence (ASACoE)
    - US Army (small group at Fort Monmouth)
  - Civil
    - DHS SwA Program
    - NIST SAMATE
    - Tactical efforts within a couple dozen organizations

1. There are a wealth of enablers available and under development to support software assurance
2. Private industry is significantly more mature than government in pursuing software assurance.
3. Government needs to better integrate software assurance into mission assurance, information assurance and acquisition
4. Government needs to move from a tactical to a strategic approach to software assurance